浅谈登陆保护系统

弦

Company LOGO

登陆系统

前言

- 一个简单的用户密码验证操作，为何会引出本次话题在登陆过程中，有哪些隐患威胁到了整个网站生态系统，本次探讨中将简单介绍如何把一个看似简单的登陆操作拆分成若干个子系统，以及各个系统之间如何运作，来保证账号的安全
- 登陆是进入系统的大门，钥匙是一个网站最具核心价值之一的账号和密码，我们该如何规划系统，让账号更加安全

内容简介

1. 验证码系统
2. 异常检测系统
3. 惩罚限制系统
4. 存储传输保护

验证码系统

- 验证码系统的由来
- 系统功能和作用
- 系统结构和组成
- 数据监控报警
- 潜在问题

验证码系统

系统由来

- 机器批量登陆行为
  - 发布垃圾信息
  - 尝试暴力破解
  - 账号合法性验证
- 人机识别技术的引入
  - 通过图形识别区分
  - 通过简单逻辑运算和语义识别区分

验证码系统

系统的功能

- 在特殊条件下拦截机器行为
- 简单机器行为的判定
- 无缝介入网站主体架构
- 生成验证码
- 判定验证码有效性

系统作用

- 防止过量错误尝试
- 防止批量试探行为
  - 正确登陆
  - 错误登陆

验证码系统

系统结构

- 用户行为预判模块
  - 调用用户历史信息
  - 根据历史信息决策
- 行为信息收集模块
  - 地理信息
  - 计数信息
- 自适应难度提升模块
  - 根据统计信息提升难度
  - 自动更换图库和字形

验证码系统

数据监控模块

- 吞吐量监控：防止系统过载，适当调整资源
- 错误率监控：防止大规模试探攻击
- 区域监控：防止区域性攻击行为
- 逃逸率监控：监控对正常用户的影响

存在的问题

- 性能瓶颈：高并发，高响应
- 压力攻击：压力过载，导致系统失效
- OCR 识别：通过机器学习等手段识别验证码
- 人肉识别：廉价任务模式，人肉识别
- 逻辑漏洞：火车订票系统 key 不失效漏洞

异常检测系统

- 异常检测系统介绍
  - 用于检测异常的登陆行为
- 系统存在的必要性
  - 异常登陆
  - 高频登陆
  - 机器登陆
- 异常检测的维度
  - 区域维度
  - 频率维度
  - 历史数据维度

异常检测系统

- 行为分析系统
  - 离线行为分析系统
    - 基于统计信息分析：区域，通过率
  - 在线实时分析系统
    - 频率
    - 失败次数
    - 区域异常数量累加

惩罚限制系统

惩罚限制系统介绍

- 为其他系统提供惩罚控制接口
- 限制异常账号的活动范围

与传统防火墙的异同

- 相同点：限制有害的行为
- 细粒度：精确到单个用户
- 精确：可以阻断一次逻辑请求

惩罚限制系统

- **系统架构支持**
  - 需要架构对惩罚的结果进行统一处理
  - 多级别惩罚机制：根据不同类型，采取不同策略
- **数据统计分析**
  - 保证系统稳定性
  - 调节系统精准度
  - 优化性能，提供高效服务

存储和传输保护

- 存储保护方案
  - 物理隔离：防止物理窃取
  - 访问控制：防止非授权访问
  - 加密存储： Hash 存储
- 传输保护介绍
  - HTTPS 传输：防止数据嗅探
  - 动态口令：双因素认证
  - 加密传输：采取可逆算法加密传输数据

Thanks

Follow Your Dream

Company LOGO